AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Terrance L. Taylor, being duly sworn, do hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge, HSI Charleston, West Virginia. During my career, I gained experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience—including on-the-job discussions with other law enforcement agents and cooperating suspects—I am familiar with the operational techniques and organizational structure of child pornography distribution networks as well as the traits and characteristics of child pornography collectors and possessors and their use of computers or other electronic and media devices to facilitate the collection, possession, trading, distribution, access and receipt of child pornographic materials.

2. I am a Special Agent with nineteen years of federal law enforcement experience. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the

Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. These areas include laws and regulations pertaining to the importation of various types of merchandise and contraband, prohibited items, money laundering, and various immigration violations. I have more specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

II. PURPOSE OF THE AFFIDAVIT

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including those properties and/or persons listed below (collectively the "SUBJECT PREMISES") for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography; 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce, which items are more specifically described in Attachment B of this Affidavit:

a. The entire property located at 60 Breezy Pl., Elkview, WV 25071 ("the SUBJECT PREMISES"), including annexes, garages, carports, the outside yard, curtilage, mailboxes, trash containers, debris boxes, sheds and outbuildings located therein;

b. The person of any residents of the SUBJECT PREMISES, as further identified in Attachment A, who are present at the SUBJECT PREMISES during the execution of the search warrant;

c. The content of computers and electronic storage devices located and seized therein;

d. The content of any locked cabinets, containers, drawers, boxes or other receptacles large enough for paper record retention or electronic storage devices located therein; and

e. Any vehicles located at the SUBJECT PREMISES.

4. Based on my training and experience and in related investigations and search warrants, and the experience of other law enforcement investigators I have communicated with, I am aware that it is common for items of digital media, including, but not limited to laptop computers, cell phones, flash drives, cameras, and digital music devices, to be transported or stored in motor vehicles. Therefore, I request the search warrant authorize the search vehicles on the subject premises that fall under the dominion or control of any resident of the SUBJECT PREMISES.

5. This Affidavit is also submitted in support of an application for a search warrant for the person(s) described in Attachment A. As set forth herein, there is probable cause to search the person of any resident of the SUBJECT PREMISES, as further described in Attachment A, who is present at the time of the execution of the search warrant for the items described in Attachment B, including cell phones and digital storage devices, such as thumb drives, that can be concealed on a person. I believe probable cause exists for the issuance of a warrant to search the residents of the SUBJECT PREMISES, as described in Attachment A, for (1) property that

constitutes evidence of a federal criminal offense; (2) contraband, the fruits of a federal crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means for committing a federal criminal offense, namely violations of Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography; 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce.

6. This affidavit is being submitted for the limited purpose of securing a search warrant and, accordingly, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause that violations of Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography; 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce, have occurred in Kanawha County, West Virginia, within the Southern District of West Virginia, and that evidence of those violations, contraband, and fruits of those violations is presently at the SUBJECT PREMISES.

III. STATUTORY AUTHORITY

7. The investigation concerns potential violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B), relating to matters involving the sexual exploitation of minors.

a. **18 U.S.C. 2252A (a)(1)** prohibits any person from knowingly mailing, transporting, or shipping child pornography in interest or foreign commerce by any means, including by computer.

b. **18 U.S.C. § 2252A(a)(2)** prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

c. **18 U.S.C § 2252A(a)(5)(B)** prohibits any person from knowingly possessing any book, magazines, periodicals films, video tapes computer disk or other matter that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means including computer, or that was produced using materials mailed, or shipped or transported in interstate or foreign commerce by any means including computer.

IV. DEFINITIONS

8. The following definitions apply to this Affidavit and its Attachments.

a. The term "**minor**," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "**sexually explicit conduct**," as used in 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "**illicit sexual conduct**" means (1) a sexual act (as defined in section 2246) with a person under 18 years of age that would be a violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United States; or (2) any commercial sex act (as defined in section 1591) with a person under the age of 18 years of age.

d. The term "**visual depiction**," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

e. The term "**computer**," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

f. The term "**child pornography**," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or

computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

g. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

h. "**Internet Service Providers**" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-locations of computers and other communications equipment.

i. "**Internet Protocol address**" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can by dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP

addresses might also be static if an ISP assigns a user's computer a particular IP address each time the computer accesses the Internet.

j. "**Domain names**" are common, easy to remember names associated with an IP address. For example, a domain name of www.usdoj.gov refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

k. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

V. BACKGROUND REGARDING COMPUTERS, CHILD PORNOGRAPHY AND THE INTERNET

10. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images

can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.[1] Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials among pornographers.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc. and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes.

[1] The File Transfer Protocol ("FTP") is a protocol that defines how files are transferred from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

VI. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER AND ELECTRONIC DEVICE SYSTEMS

11. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

12. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or

"footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

13. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a) Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b) Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c) The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d) Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly

unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

14. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a) The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b) In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit ("CPU"). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

15. As described further in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other

storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), of any device located within the SUBJECT PREMISES.

16. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b) Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d) Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

17. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b) Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c) The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

d) Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts,

electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

e) Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

f) Moreover, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

j) I know that when an individual uses a computer to distribute or attempt to distribute child pornography, the individual's computer will generally serve

both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

18. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

19. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

20. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and its attachments, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine

whether it is evidence described by the warrant.

VII. BIOMETRIC ACCESS TO DEVICES

21. This warrant permits law enforcement to compel individuals located at the SUBJECT PREMISES to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

22. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

23. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the

front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

24. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

25. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

26. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

27. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

28. As set forth in further detail below, there is probable cause to believe that an individual residing at the SUBJECT PREMISES is involved in federal crimes related to child pornography. There is also probable cause to believe that more than one individual resides at the residence. As the currently-available information does not precisely identify which individual residing at the SUBJECT PREMISES was involved in the possession, transport, receipt, and/or distribution of child pornography, it is necessary for this search warrant to authorize law enforcement to compel any and all individuals present at the SUBJECT PREMISES to provide biometric access to any devices subject to seizure that may be unlocked using biometric features.

29. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the

fingers (including thumbs) of individuals located at the SUBJECT PREMISES to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of the face of individuals located at the SUBJECT PREMISES and activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the face of individuals located at the SUBJECT PREMISES and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that individuals located at the SUBJECT PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel individuals located at the SUBJECT PREMISES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

VIII. BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE

30. Based on my training and experience, and publicly available information, I know that the National Center for Missing and Exploited Children ("NCMEC") is a nonprofit, nongovernmental organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

31. In addition to reports from the general public, Title 18, United States Code, Section 2258A requires all providers of an electronic communication service or remote computing service

to the public through a facility or means of interstate or foreign commerce, known as electronic service providers ("ESPs"), to report "apparent child pornography" to NCMEC via the CyberTipline. Leads received by NCMEC are reviewed by specially trained analysts, who examine and evaluate the reported content, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation. In this case, the ESP was MediaLab/Kik and it made a CyberTipline referral ("CyberTip") to NCMEC based on the conduct described below.

32. Thus, NCMEC received CyberTips on the following types of criminal conduct: possession, manufacture and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

33. CyberTips can vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an electronic communication service or remote commuting service uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. See 18

U.S.C. § 2258A(b). Also, as will be illustrated below, CyberTips can be supplemented and made in connection with other CyberTips.

IX. BACKGROUND ON KIK MESSENGER

34. Kik Messenger is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

35. Kik Messenger users are also able to create chat groups, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik Messenger users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

X. CHARACTERISTICS OF PERSONS WHO COLLECT OR TRAFFIC CHILD PORNOGRAPHY

36. Your affiant has experience in assisting with, and leading, investigations into child pornography. Your affiant has conducted investigations into those who solicit and share child pornography by electronic means. Your affiant has worked with other law enforcement agencies

to conduct logical investigations into those who solicit, share and otherwise engage in activity related to child pornography.

37. As a result of the aforementioned knowledge and experience, your affiant has learned that the characteristics described in this affidavit are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material may include, but is not limited to, photographs, negatives, slides, magazines, printed media, motion pictures, video tapes, books and other media stored electronically on computers, digital devices or related digital storage media.

38. Offenders who deal with the above-referenced child pornography material depicting minors engaged in sexually explicit conduct obtain or traffic in such materials through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

a. Downloading via the Internet and other computer networks (including from websites, peer-to-peer file sharing networks, news groups, electronic bulletin boards, chat rooms, instant message conversations, internet relay chats, email).

b. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer.

c. Trading with other persons with similar interests through electronic transfer, shipments or deliveries.

39. These offenders collect materials depicting minors engaged in sexually explicit conduct for many reasons. These reasons include the following:

a. For sexual arousal and sexual gratification.

b. To facilitate sexual fantasies in the same manner that other persons utilize adult pornography.

c. As a medium of exchange in return for new images and video depicting minors engaged in sexually explicit conduct.

40. These offenders often view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Subsequently, these offenders prefer not to be without their child pornographic material for any prolonged period of time and often go to great lengths to conceal and protect their illicit collections from discovery, theft or damage. To safeguard their illicit materials, these offenders may employ the following methods:

a. The use of Internet-based data storage services, such a Google Drive.

b. The use of labels containing false, misleading or no title.

c. The application of technologies, software and other electronic means such as encryption, steganography (the practice of concealing a file, message, image, or video within another file, message, image, or video), partitioned hard drives, and misleading or purposefully-disguised applications on electronic devices.

d. The use of safes, safety deposit boxes or other locked or concealed compartments within premises or structures that the offender controls.

XI. FACTS ESTABLISHING PROBABLE CAUSE

41. On or about August 22, 2021, MediaLab/Kik submitted CyberTip Report 98779073 to the NCMEC CyberTipline. The CyberTip Report was the result of MediaLab/Kik representatives reporting to NCMEC that a Kik profile bearing the username "jsparrow2174" had uploaded eight (8) videos and one (1) image through Kik Messenger. Kik representatives viewed the aforementioned files and found them to contain depictions of prepubescent and pubescent minors engaged in sexual activity. Kik representatives advised the aforementioned files were sent from "jsparrow2174."

42. In Cybertip Report 98779073, MediaLab/Kik reported the following information regarding Kik user "jsparrow2174" uploading eight videos and one image of apparent child pornography between on or about July 13, 2021, and on or about July 16, 2021:

Email Address: ultimatew31@gmail.com

Screen/User Name: jsparrow2174

IP Address: 47.220.40.206 on 08-19-2021 at 21:35:46 UTC

NCMEC Geo-Lookup: Elkview, WV, Suddenlink Communications

43. On or about September 22, 2021, your Affiant reviewed the following video files associated to CyberTip 98779073 and found those to depict the following:

a. Alphanumeric file 86241aa7-cb32-466f-8f87-cb4f259e72a3.mp4 was uploaded on July 13, 2021, at 23:40:35 UTC from IP address 47.220.40.206 associated to Suddenlink Communications. The 50-second video depicts a nude, prepubescent female with white skin, approximately 9-12 years old. The prepubescent female is lying on her back with her knees pulled up while an adult, white male penetrates her anus with his erect penis.

b. Alphanumeric file 7547bd98-4068-4359-acdd-d2047e110ca3.mp4 was uploaded July 13, 2021, at 23:43:39 UTC from IP address 47.220.40.206 associated to Suddenlink Communications. The 1 minute, 41 second video depicts a nude, prepubescent female approximately 9-12 years old. The nude, prepubescent white female with brown hair is on her hands and knees while an adult, white male penetrates her vagina with his erect penis from behind.

c. Alphanumeric file e6b04eba-9d47-4263-963b-72323b708aff.mp4 was uploaded on July 16, 2021, at 04:37:30 UTC from IP address 47.220.40.206 associated to Suddenlink Communications. The 49-second video depicts a nude, prepubescent female with white skin and blonde hair taking a video of herself. The nude, prepubescent female penetrates her anus with a "sharpie" marker. The female also digitally penetrates her vagina with her fingers.

44. On or about September 16, 2021, HSI Charleston issued an administrative subpoena/summons to Suddenlink Communications regarding subscriber information pertaining to IP address 47.220.40.206 on July 13, 2021, through July 16, 2021. A review of the results obtained on October 18, 2021, identified the following subscriber information: Terry ROATSEY,

60 Breezy Pl., Elkview, WV, (SUBJECT PREMISES) and an activation date of April 20, 2005. According to publicly available records, Terry ROATSEY, approximately age 73, is believed to be the father of Todd Christopher ROATSEY, approximately age 42; furthermore, Terry ROATSEY owned the aforementioned property prior to Todd ROATSEY purchasing the SUBJECT PREMISES on April 5, 2007.

45. Publicly available database checks revealed that Terry ROATSEY and Todd ROATSEY both appear to reside at the SUBJECT PREMISES. According to the Kanawha County Assessor's Office, the SUBJECT PREMISES, legal description Unnumbered LT 209X71 Reedmont Acres, Parcel #15-38A002100010000, Account #07314685, is owned by Todd ROATSEY.

XII. CONCLUSION

46. Based on the foregoing, I respectfully submit that there is probable cause to believe that a person residing at the SUBJECT PREMISES has violated the federal criminal statutes cited herein, and that contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this affidavit, are located at the SUBJECT PREMISES, described in Attachment A.

47. Your affiant, therefore, respectfully requests that the Court issue a search warrant for the SUBBJECT PREMISES; the content of computers and electronic storage devices located and seized therein; content of any locked cabinets, containers, drawers, boxes or other receptacles large enough for paper record retention or electronic storage devices located therein; the person of any resident of the SUBJECT PREMISES who is located at the SUBJECT PREMISES, and any

vehicles located at the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

Further your affiant sayeth not.

SPECIAL AGENT TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Signed and sworn to by telephonic means on this 27th day of October, 2021:

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE